IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF: 47 PORTLAND STREET, APT. 1, LANCASTER, NEW HAMPSHIRE; AND THE PERSON OF ISAIAH LAFOE.	Case No. 22-mj-196-01-AJ Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, **Rebecca Gworek**, being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search (A) the premises and property located at 47 Portland Street, Apt. 1, Lancaster, New Hampshire (the "SUBJECT PREMISES"), to include all rooms, attics, closed containers, and other places therein, including garages, storage areas, utility sheds, mailboxes, and trash containers under the control of the occupants of the residence, (B) the person of ISAIAH LAFOE, and (C) any computers, cellular telephones, tablets, computer equipment, computer storage media and electronic storage media found during the course of said searches. Located within the places and items to be searched, I seek to seize evidence, fruits, and instrumentalities relating to violations of 18 U.S.C. §§ 2422(b) [Coercion and Enticement of a Minor], 2251(a) [Production of Child Pornography], 2252A(a)(2) [Receipt of Child Pornography], 2252A(a)(5) [Possession of Child Pornography], and 1470 [Transfer of Obscene Material to a Minor] (the "Subject Offenses"), as more fully described in Attachment B.

2. I am an investigator with the Federal Bureau of Investigation (FBI) and have been since January 2016. I am assigned full-time to the Albany Division, Albany, N.Y. I have investigated a variety of violent crimes including violent gangs, domestic terrorism, child sexual

exploitation and assault. My current duties include investigating criminal violations relating to child exploitation and child pornography, including violations pertaining to the enticement and coercion, as well as production, distribution, receipt, and possession of child pornography. I have gained experience regarding such crimes through training in seminars, classes and everyday work related to conducting these times of investigations. I have observed and reviewed numerous examples of child pornography in all forms of media including computer media. My investigative experience includes interviewing victims and witnesses, as well as conducting searches of physical locations, social media, and electronic devices, as well as use of location information to identify and locate criminals.

3. I have received training in the area of Child Sexual Abuse Material (CSAM) and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, and I am authorized by law to request a search warrant.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of the Subject Offenses have been committed, are being committed, and will be committed by ISAIAH LAFOE. There is also probable cause to believe that evidence, contraband, fruits, and instrumentalities of the Subject Offenses are at the SUBJECT PREMISES.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer

hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the internet service provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

g. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including

access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

h. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

i. "Records," "documents," and "materials," as used herein, include all information recorded in any form and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

j. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

k. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

PROBABLE CAUSE

7. The United States, including the FBI, is conducting a criminal investigation of ISAIAH LAFOE for potential violations of 18 U.S.C. §§ 2422(b) [Coercion and Enticement of a Minor], 2251(a) [Production of Child Pornography], 2252A(a)(2) [Receipt of Child Pornography], 2252A(a)(5) [Possession of Child Pornography], and 1470 [Transfer of Obscene Material to a

Minor] (the Subject Offenses). Between December 2020 and March 2021, Lafoe, aged 22 years old at the time, communicated with a then 13-year-old girl ("Victim-1") via social media, including Google Duo, as well text message and Victim-1 had sent Lafoe sexually explicit nude images of herself. A 13-year-old boy in Reno, Nevada ("Victim-2") reportedly also communicated with LaFoe in the summer of 2021. Based on the FBI's investigation, there is probable cause to believe that Lafoe resides and has logged on to the internet from the SUBJECT PREMISES. There is probable cause to believe that the SUBJECT PREMISES and the person of ISAIAH LAFOE contains evidence, fruits, contraband and instrumentalities of the Subject Offenses, including communications related to the coercion and enticement of minors, and images of child pornography that were produced by minors as a result of his enticement and coercion of them.

Victim-1

8. In late February 2021, a 13-year-old girl (Victim-1) and her mother, both residents of Troy, New York, reported to the Troy Police Department that Victim-1 had been coerced into sending sexually explicit images to an adult male. During the initial interview, Victim-1 reported the following:

a. In December 2020, Victim-1 discovered an online website called Omegle.[1] Using Omegle, Victim-1 met at least three males who she eventually befriended on another social media application, Snapchat. According to Victim-1, she sent sexually explicit photographs to each male via Snapchat. One male in particular—which was listed as "DB" in the contacts on Victim-

[1] Omegle is a free online chat website that allows users to socialize with others without the need to register. The service randomly pairs users in one-on-one chat sessions where they chat anonymously using the names "You" and "Stranger."

1's phone—talked to Victim-1 frequently until Victim-1's mother went through Victim-1's phone and took it from her days prior to reporting to the police. According to Victim-1, the contact listed in her phone as "DB" spoke with her via Snapchat, Google Duo, and via phone. Victim-1 stated that the person she communicated with, listed in her phone as "DB," was named Isaiah Lafoe.

b. According to Victim-1, Lafoe also contacted her via TikTok and identified Lafoe's TikTok profile photo as the person she routinely spoke to. According to Victim-1, when she initially met Lafoe online, Lafoe presented himself as being 15 but later informed Victim-1 that he was 19. Lafoe informed Victim-1 that he wanted to meet her, but they had to wait until Victim was eighteen years old. During the conversations, Lafoe told Victim-1 that he resided in New Hampshire at an undisclosed address.

c. Victim-1 and her mother consented to the search of Victim-1's phone, which was subsequently searched by law enforcement and was confirmed to contain images of child pornography.

9. On March 1, 2021, the FBI interviewed Victim-1 at her residence in Troy, New York. During the interview, Victim-1 reported the following:

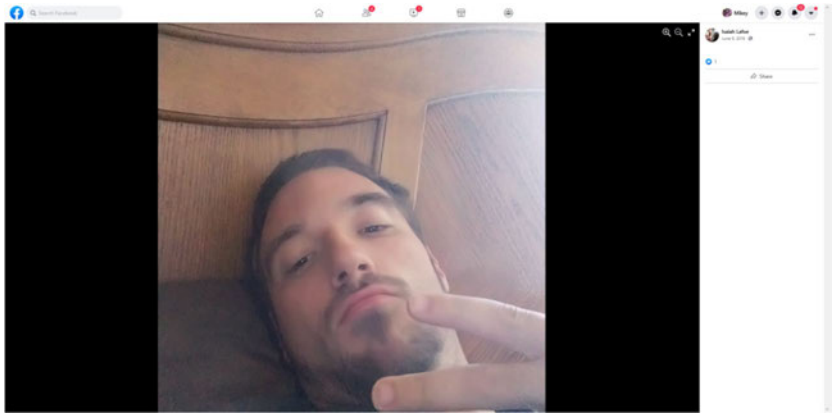
a. Victim-1 confirmed that she met Lafoe via Omegle in December 2020. When Victim-1 asked the user later identified as Lafoe how old he was, Lafoe initially stated that he was fifteen. After Victim-1 confirmed that she was 13 years old, Lafoe asked her to transition to another social media platform, Snapchat.

b. Victim-1 and Lafoe then transitioned to Snapchat where they had further communications, which were saved on her phone. According to Victim-1, Lafoe made her believe she could trust him and then transition to a phone number to text. They also used Google Duo[2] to video chat. According to Victim-1, Lafoe made Victim-1 feel safe and informed her that he was 15 years old. Lafoe told her his name was Isaiah Lafoe and left his name on voicemails saved on Victim-1's phone, which law enforcement has reviewed and confirmed.

c. Victim-1 also stated that Lafoe told her that her body was no longer hers and that she could not be with anyone else. Lafoe asked Victim-1 to call him "daddy." When Victim-1 refused to send images or chat with him, Lafoe would curse at her in Spanish and scream at her via text.

d. Victim-1 also provided a description of Lafoe matching the description known to law enforcement for Lafoe by describing Lafoe as a white male with facial hair and a tattoo on his left arm with his grandmother's name. The following image was shown to Victim-1 of LaFoe, which Victim-1 positively identified as Lafoe and was the same male she had been video chatting, texting, and communicating with and was the same male who had asked her for sexually explicit and lascivious images:

[2] Google Duo is a proprietary voice over IP (VoIP) and videotelephony service developed by Google, available for Android, iOS and web browsers that lets users make and receive one-to-one and group audio and video calls with other Duo users in high definition, using end-to-end encryption by default. Duo can be used either with a phone number or a Google account, allowing users to call someone from their contact list.



e. According to Victim-1, Lafoe sent Victim-1 images of his penis via text and Snapchat and then would call her to see if she had seen the image.

f. When asked about the images she sent to Lafoe, Victim-1 reported that Lafoe "roped" her into making the images and asked her very sweetly and promised not to show anyone else. Initially, Victim-1 sent images of herself in outfits, and then, after Lafoe made her more comfortable, she sent images of her breasts and vagina. Victim-1 started with still photographs and then transitioned to videos. The videos were made with her phone and sent via Snapchat and Google Duo.

g. When asked about the progression of the production of the videos, Victim-1 reported that Lafoe asked for more and more photos and stated that she trusted him. Victim-1 reported that some of the videos depicted Victim-1 masturbating and doing whatever made Lafoe feel good. Victim-1 also confirmed that Lafoe made her use an object in her vagina to masturbate. Victim-1 reported feeling disgusted after making the videos.

h. When Lafoe instructed her to produce and send images, Victim-1 understood that Lafoe was in his residence in New Hampshire. Lafoe told her that he lived in New Hampshire but did not specify where, though he mentioned that he was staying with his mother. When Victim-1 asked about whether Lafoe would travel to New York, Lafoe told her that he would come to see her when she was 18 years old. Victim-1 told Lafoe she lived in Albany, New York during their conversations and her location was visible in her online profiles as being in Troy, New York. Lafoe told Victim-1 that he was not working and that he used to be in a gang. Victim-1 reported that all of the videos and images she created for Lafoe were produced in Troy, New York at her house.

i. Victim-1 reported that she communicated with Lafoe via phone and he was using phone number [redacted]2010 ("Target Cell Phone 1").

10. Law enforcement has performed a forensic review of the phone recovered from Victim-1 and has confirmed that there are images and videos of child pornography on that device. All of these image files are available for the Court's review upon request. Below are descriptions of three images found in the files on Victim-1's phone that Victim-1 stated were produced at Lafoe's request:

a. A close-up photo of the Victim-1's vagina.

b. A close-up photo of Victim-1's anus and vagina with her hand/fingers inside her vagina.

c. A close-up photo of Victim-1's hand on her vagina.

11. Records from Verizon Wireless show that the phone number [redacted]2010 (Target Cell Phone 1) has a listed subscriber with initials A.M. with an address at 47 Portland Street #1, Lancaster, New Hampshire (the **SUBJECT PREMISES**).

12. Records from the New Hampshire Department of Motor Vehicles show that Isaiah Lafoe has a driver's license with an address located at 47 Portland Street, Apt. 1, Lancaster, New Hampshire (the **SUBJECT PREMISES**).

Additional Information Related to Lafoe

13. Records from Microsoft Corporation, dated May 3, 2021, show that a Microsoft account was registered to "Isaiah Lafoe" (the "Lafoe Microsoft Account"), with an associated address at 47 Portland Street, Lancaster, New Hampshire (the **SUBJECT PREMISES**). The Lafoe Microsoft Account listed an email address of [redacted]@]gmail.com (the Lafoe Gmail Account) and listed the following as an active device associated with the Account: a Samsung Galaxy S6 Black 32GB phone with IMEI [redacted]6567 and IMSI [redacted]0162. The Lafoe Microsoft Account was associated with Xbox gaming activity, including IP activity under gamer tag "Havokofdis98" between February 11, 2021, to April 11, 2021, using IP address 67.253.52.0., which is associated with a subscriber with initials D.H. at an address in Lancaster, New Hampshire.

14. Meta Platforms, Inc. records show that the Facebook account with vanity name isaiah.lafoe.16 was registered in the name of Isaiah Lafoe on October 20, 2020 and registered with the email account [redacted][@]gmail.com (the Lafoe Gmail Account).

15. Snap, Inc. records show that a Snapchat account with username "i_lafoe20" was created on September 4 with display name "Isaiah Lafoe." A phone number [redacted]7922 was listed under the account and as of July 2022, the account remained active.

Victim-2

16. On or about July 28, 2021, a 13-year-old boy located in Reno, Nevada ("Victim-2"), through his mother, reported to NCMEC that he had been communicating with an individual named "Isaiah" at an unknown address in New Hampshire for the previous three months. Victim-2 reported that "Isaiah" had communicated with him using mobile phone number [redacted]5558 ("Target Cell Phone 2"). Victim-2 reportedly met "Isaiah" while playing an online game called "Call of Duty."[3] According to Victim-2's mother, "Isaiah" had been grooming Victim-2 and turned him into a girl; the child was no longer acting like himself as a boy would and had been acting like his sisters around the house. "Isaiah" had reported called Victim-2 "bae" and "wifey" and told Victim-2 that they were engaged and that he was going to "come for him and marry him." Victim-2 and "Isaiah" video chatted on Google Duo and the social media application TikTok. Victim-2's mother reported that Victim-2 had exchanged photos with "Isaiah" but did not know if the child sent real photos of himself.

17. Records from Verizon Wireless show that the phone number [redacted]5558 (Target Cell Phone 2) has a listed subscriber of "Isaiah Lafoe" with an address at 47 Portland Street, Lancaster, New Hampshire (the **SUBJECT PREMISES**).

[3] Based on my training and experience, the online game "Call of Duty" can be played using online gaming platforms such as Xbox.

Undercover Activity

18. On October 29, 2021, an officer acting in an undercover capacity utilizing the persona of a thirteen-year-old male (the "UC") investigated the Microsoft Xbox gaming platform associated with gamertag "Havokodis98," which is linked to the Lafoe Gmail Account as noted above. The UC sent a friend request to the user of Havokodis98, which was promptly accepted. The user of the Havokodis98 account replied with a message to the UC stating, "I can't hear you." The UC then utilized an audio capable headset and made voice contact with "Havokodis98." Through the conversation, the user of the Havokodis98 account stated that his name was "Isaiah," that he was 23 years old and stated that he was currently located in Concord, New Hampshire. "Havokodis98" provided his cellular telephone number as [redacted]558 (Target Cell Phone 2) and requested that the UC send him a text message.

19. On July 13, 2022, an officer acting in an undercover capacity further investigated the Xbox gaming platform associated with gamertag "Havokodis98." As of July 13, 2022, the Xbox account for gamertag "Havokodis98" was still active and the profile photo on the account matched available photographs and the description for Isaiah Lafoe.

The Lafoe Gmail Account

20. Records from Google LLC show that Lafoe Gmail Account was registered in the name of "Isaiah Lafoe" on October 20, 2020. According to records from Google, the Lafoe Gmail Account listed phone number [redacted]3620 ("Target Cell Phone 3") as both a recovery SMS number and as a Sign-in Phone number and listed IP activity associated with 67.253.52.249.

21. Records from T-Mobile show that the phone number [redacted]3620 (Target Cell Phone 3, associated with the Lafoe Gmail Account) was active and had made calls between December 25, 2020, and March 25, 2021.

22. Google IP records produced in response to an order authorizing the installation and use of a pen registered and trap and trace device for the Lafoe Gmail Account shows that there was a login to the Lafoe Gmail Account from IP address 67.253.52.249 on July 23, 2022.

23. Charter Communications records show that IP address 67.253.52.249 was registered to a subscriber with initials T.D. with a listed address of 47 Portland Street, Apt. 1, Lancaster, New Hampshire (the **SUBJECT PREMISES**), as of July 23, 2022. The subscriber T.D. is believed to be Isaiah Lafoe's mother.

Surveillance

24. On September 13, 2021, physical surveillance was conducted in the vicinity of 47 Portland Street, Lancaster New Hampshire (the SUBJECT PREMISES), and 1 1st Street, Lancaster, New Hampshire. A red Ford F-150 bearing NH license plate (the "Red Ford F-150"), was observed near 47 Portland Street, and a black Ford Fiesta bearing NH license plate, registered to D.H. (the "Black Ford Fiesta"), was observed parked and unoccupied near 1 1st Street. Lafoe was not observed during the surveillance, which lasted from approximately 7:55 am to 11:00 am.

25. On September 15, 2021, physical surveillance was conducted in the vicinity of 47 Portland Street, Lancaster New Hampshire (the SUBJECT PREMISES), and 1 1st Street, Lancaster, New Hampshire. The Red Ford F-150 was observed near 47 Portland Street and the Black Ford Fiesta was observed near 1 1st Street, both of which were parked and unoccupied. 47

Portland Street is located on a busy thoroughfare, making continued surveillance difficult for law enforcement. Lafoe was not observed during the surveillance, which lasted from approximately 7:25 am to 1:00 pm.

26. On September 1, 2022, physical surveillance was conducted in the vicinity of 47 Portland Street, Lancaster, New Hampshire, which appears to be a three-story multi-family residence with at least two separate entrances. The front door appears to belong to Apartment #2. During surveillance, agents observed Lafoe entering/exiting the residence via a white door on the right side of the residence, and agents believe that this side door leads to the SUBJECT PREMISES. The entrance to the SUBJECT PREMISES is circled in the following photograph:

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

27. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically

serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images

or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person. Your Affiant therefore also requests permission to search the person of ISAIAH LAFOE for such evidence.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file

on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

28. In my training and experience, people tend to carry their cellular telephones on their person even when physically inside their homes. As discussed in more detail below, in my training and experience, individuals that use an online gaming system or via social media to induce or entice a child to create and send sexually explicit images (like there is probable cause to be believe LAFOE did) typically do so using their cellular telephones and/or transfer copies of the child pornography files they obtain to their cellular phones because they want ready access to the material for sexual gratification and because they consider their personal cellular telephones to be more secure than tablets and personal computers that might be shared with others in a home.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

29. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. They may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often

maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis; however, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[4]

f. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if a user uses a portable device (such as a mobile phone) to

[4] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home.

g. Individuals who collect child pornography also often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica. They do this to gain status, trust, acceptance and support and to increase their collection of illicit images and child erotica. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, peer-to-peer (P2P) chat and file sharing programs, e-mail, e-mail groups, bulletin boards, Internet Relay Chat (IRC), newsgroups, Internet clubs, and various forms of Instant Messaging such as Google Hangouts, which can be saved on the users' computer or other digital storage media.

h. Besides sexual photos of minors and child erotica, such individuals often produce and/or collect other written material on the subject of sexual activities with minors, which range from fantasy stories to medical, sociological, and psychological writings, which they save to understand and justify their illicit behavior and desires.

i. Individuals who collect child pornography often collect, read, copy or maintain names, addresses, including e-mail addresses, phone numbers, and lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests, or have child pornography and child erotica for sale or trade. These contacts are maintained for personal referral, exchange or, sometimes, commercial profit. They may maintain these names on computer storage devices, web sites or other Internet addresses, and their discovery can serve as leads to assist law enforcement in proving the instant case and in apprehending others involved in the underground trafficking of child pornography.

j. Individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect their collections of these materials from discovery, theft, and damage. The known desire of such individuals to retain child pornography, together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other security measures, save it on movable media such as CD's, DVD's, flash memory, thumb drives, and removable hard drives (which can be as small as a postage stamp and easily hidden), or send it to third party image storage sites via the Internet.

30. Based on the following, I believe that LAFOE likely displays characteristics common to individuals who produce, receive, distribute, possess and access with intent to view child pornography.

***

31. Based on my training and experience, and the evidence developed in this case and described above, there is probable cause to believe that LAFOE used the PREMISES to commit or facilitate the commission of the Subject Offenses; further, based on the nature of child pornography evidence, and the way such evidence is created, distributed and stored, there is probable cause to believe that evidence of LAFOE's criminal conduct involving Victim-1 will be found at the SUBJECT PREMISES, and within and on LAFOE's person.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

32. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES and on the person of ISAIAH LAFOE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

33. I submit that if a computer or storage medium is found during the searches authorized by this warrant, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have

been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

34. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES and on the person of ISAIAH LAFOE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

c. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

d. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

e. The process of identifying the exact files, pieces, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

f. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

g. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain the following: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved;

records of Internet discussions about the crime; and other records that indicate the nature of the offense.

35. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy

or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort

through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

36. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

37. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might

expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

38. Based on my training and experience, it is likely that the SUBJECT PREMISES will contain at least one mobile or storage device, such as an iPhone or Android device, that can be used to store, send, receive, distribute, and possess child pornography and can be used to communicate regarding child pornography as well as to communicate with minors to coerce them into sexually explicit conduct.

39. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize. The proposed warrant would permit law enforcement to compel LAFOE to unlock any electronic device requiring biometric access, if that device is found during the search.

40. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home"

button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

41. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

42. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

43. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's

contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

44. As discussed above, I believe that one or more digital devices and/or computers will be found during the search. The passcode or password that would unlock the device subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

45. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

46. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose

fingerprints are among those that will unlock the device via biometrics, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the SUBJECT PREMISES to press their finger(s) against the sensors of the locked device(s) found during the search of the SUBJECT PREMISES in order to attempt to identify the device's user(s) and unlock the device(s) via biometric features.

47. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant at the SUBJECT PREMISES, or on the person of ISAIAH LAFOE, and may be unlocked using one of the aforementioned biometric features, the proposed warrant would permit law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of LAFOE to the fingerprint scanner of the devices; (2) hold the devices in front of the face of LAFOE and activate the facial recognition feature; and/or (3) hold the devices in front of the face of LAFOE and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrants do not authorize law enforcement to request that any individual state or otherwise provide the password or any other means that may be used to unlock or access any device. Moreover, the proposed warrant does not authorize law enforcement to ask such persons to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION

48. Based on the above, there is probable cause to believe that LAFOE has committed the Subject Offenses, and that a search of the PREMISES, the person of LAFOE, and any electronic devices located therein, will reveal evidence, contraband, fruits of crime, or other items illegally possessed concerning the Subject Offenses. Therefore, I respectfully request that the Court authorize the referenced search warrant in this matter.

49. This authorization includes the authority to search any cell phones, computers, computer equipment, or computer storage media and electronic storage media located during the searches of the SUBJECT PREMISES and the person of LAFOE.

Attested to by the Affiant:

/s/ Rebecca Gworek
Rebecca Gworek, Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. P. 41 and affirmed under oath the contents of this affidavit and application.

Date: September 9, 2022

/s/ Andrea K. Johnstone
Hon. Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

PLACES AND ITEMS TO BE SEARCHED

The places and items to be searched are (A) the premises and property located at 47 Portland Street, Apt. 1, Lancaster, New Hampshire 03584 ("SUBJECT PREMISES"), to include all rooms, attics, closed containers, and other places therein, including garages, storage areas, utility sheds, mailboxes, and trash containers under the control of the occupants of the residence, (B) the person of ISAIAH LAFOE, and (C) any computers, cellular telephones, tablets, computer equipment, computer storage media and electronic storage media found during said searches.

The SUBJECT PREMISES is depicted below and described as a white three-story house, with a covered front porch. From the street, the entrance to the SUBJECT PREMISES is a door on the right side of the house, which is circled in the following photograph:

The person of ISAIAH LAFOE is depicted below:

ATTACHMENT B

ITEMS TO BE SEIZED AND SEARCHED

The items to be seized includes all information and objects that constitute fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 2422(b) [Coercion and Enticement of a Minor], 2251(a) [Production of Child Pornography], 2252A(a)(2) [Receipt of Child Pornography], 2252A(a)(5) [Possession of Child Pornography], and 1470 [Transfer of Obscene Material to a Minor] (the "Subject Offenses") by ISAIAH LAFOE:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. Evidence of the lack of such malicious software;

d. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. Evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. Evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. Evidence of the times the COMPUTER was used;

i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. Records of or information about Internet Protocol addresses used by the COMPUTER;

l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. Contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.
4. Child pornography child erotica, and other images of children, including photographs, drawings, sketches, fantasy writings, and notes showing an interest in unlawful sexual contact with children, and evidence assistance authorities in identifying any such children;
5. Evidence of correspondence and images sent and received between LAFOE and any minor, including chats, images, videos, and text messages of minors;
6. Clothing, personal belongings, gifts, sexual toys, lubricants, devices and articles, which may be used to engage in sexually explicit conduct with minors or to entice minors to engage in sexually explicit conduct, or receipts of any such purchases;
7. Internet history, including evidence of visits to websites and applications that offer visual depictions of minors engaged in sexually explicit conduct or that offer a platform to communicate with others who are interested in unlawful sexual contact with children;
8. Correspondence and records regarding engaging in, or enticing others to engage in sexually explicit conduct with minors, including envelopes, letters, mailings, electronic mail, chat logs, electronic messages on messaging applications such as Wickr and Whisper, books, ledgers, and records of communications with other individuals, including on any child exploitation bulletin boards, chat forums, or organizations;
9. Notes, documents, records, invoices, or correspondence, in any format and medium, including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information, and handwritten notes, related to the coercion and enticement of minors, the production, receipt, distribution, and/or possession of child pornography;

10. Diaries, address books, notebooks, names, and lists of names and addresses of individuals (including minors);
11. Envelopes, letters, mailings, books, ledgers, and records of communications, including electronic messages such as chats and e-mail with other individuals, including on any child exploitation bulletin boards, chat forums, or organizations;
12. Records related to the use of social media platforms, including Google Duo, Snapchat, Facebook, Instagram, and TikTok;
13. Records related to the use of aliases such as "DB" or "Havokodis98"
14. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;
15. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
16. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

Biometric Access. During the execution of the search of the SUBJECT PREMISES and the person of ISAIAH LAFOE, as described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of LAFOE, (2) hold the devices in front of the face of LAFOE and activate the facial recognition feature; and/or (3) hold the devices in front of the face of LAFOE found on LAFOE's person and/or at the SUBJECT PREMISES, and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.